

Problema de conectividade de túnel IPsec de acesso seguro com o roteador Versa Networks devido à negociação ESN

Contents

Problema

Durante a implantação do Cisco Secure Access em uma filial usando o Roteador Versa-Network como o dispositivo de borda, problemas de conectividade foram encontrados apesar de ambos os túneis IPsec parecerem operacionais. T

Os sintomas específicos incluíram:

- Sem conectividade da filial com o Cisco Secure Access
- Acesso à Internet através de rotas estáticas não funcionando
- Tráfego criptografado unidirecional observado (saída somente para acesso seguro)
- Estatísticas do roteador mostrando pacotes de saída sendo enviados, mas nenhum pacote de entrada recebido
- Detecção de ponto morto funcionando bidirecionalmente entre o roteador SD-WAN e o acesso seguro
- Valores do Índice de Parâmetros de Segurança (SPI) para correspondência correta do tráfego de saída
- A oscilação de túnel (redefinição) não resolveu o problema de conectividade
- Capturas de pacotes e capturas de tela confirmaram a falta de tráfego de entrada
- A alteração de cifras de túnel de CBC para GCM não resolveu o problema

A investigação revelou que o tráfego não estava conseguindo descriptografar no lado da Cisco devido a erros de checksum, que foram rastreados para o roteador Versa que está negociando a funcionalidade ESN (Extended Sequence Number).

Ambiente

- Implantação do Cisco Secure Access
- Roteador Versa-Networks como dispositivo de borda
- Configuração de túnel IP-Identity
- Configuração de túnel IPsec com tentativas de cifra CBC e GCM

Resolução

A resolução envolvia a desabilitação da negociação do Extended Sequence Number (ESN) no roteador Versa para evitar erros de checksum que estavam causando falhas decriptografia no headend do Cisco Secure Access.

Etapas a serem resolvidas

Passo 1: Identificar a causa raiz

A investigação determinou que o roteador Versa estava negociando o ESN (Extended Sequence Number, número de sequência estendido), o que estava fazendo com que o headend do Cisco Secure Access recebesse erros de checksum e falhasse ao descriptografar pacotes criados pelo ESN.

Passo 2: Desative o ESN no roteador Versa

Entre em contato com o suporte da Versa Networks ou com o administrador do roteador para desativar as verificações e a negociação de ESN na configuração do roteador Versa. Isso aborda o bug Versa conhecido que faz com que o ESN seja negociado incorretamente.

Passo 3: Verificar a conectividade

Depois de desabilitar a negociação ESN, confirme se o fluxo de tráfego bidirecional está estabelecido e se a conectividade total da filial para o acesso seguro e a Internet foi restaurada.

Passo 4: Monitore o fluxo de tráfego

Verifique se as estatísticas de pacotes de entrada e de saída no Roteador mostram o fluxo de tráfego adequado em ambas as direções, confirmando a resolução bem-sucedida do problema de tráfego unidirecional.

Causa

A causa raiz foi identificada como um bug conhecido do Versa Networks (ID do bug de suporte do Versa: 122437 - O ESN não deve ser negociado pelo VOS) onde o roteador Versa negocia incorretamente a funcionalidade do Extended Sequence Number (ESN) durante o estabelecimento do túnel IPsec. Essa negociação ESN faz com que o headend do Cisco Secure Access receba pacotes com erros de checksum, evitando a descryptografia adequada e resultando em fluxo de tráfego unidirecional. O roteador Versa envia pacotes de saída com êxito, mas o tráfego de retorno não pode ser processado corretamente devido às falhas de descryptografia relacionadas ao ESN.

Conteúdo relacionado

- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.